Remarks of
U.S. Representative Edward J. Markey (D-MA)
Ranking Democrat, House Subcommittee on
Telecommunications, Trade, and Consumer Protection
Computers, Freedom, and Privacy Conference
Washington, D.C.

April 7, 1999

[Thank you. I want to thank you for inviting me to speak today and thank Marc Rotenberg for graciously accommodating the schedule...]

As everyone knows, the U.S. and NATO are currently engaged in military action in Kosovo against the Serbs. According to many accounts, the Serbs are in the process of emptying out villages in Kosovo of their ethnic Albanian inhabitants. Many ethnic Albanians are being killed and thousands more are either in hiding or on the run and fleeing to border areas.

I mention this to all of you not to simply make note of the grim reality of current events, but because I think it is helpful to remind ourselves of a few things when thinking about privacy and freedom. First, we can observe quite readily on TV and on the news sites on the Net that great harm is being done to people in Kosovo based upon their ethnicity, their religious affiliation, upon what village they may hail from, or who their parents may be. Right now, in many parts of the former Yugoslavia, information about who you are could literally mean whether you are safe or in grave personal peril. This is such a depressing situation because this is not a story from the Middle Ages or Nazi Germany - this is post-Cold War Europe in 1999.

When people from the European Community tell us that they see privacy policy not merely through the prism of trade relations but as a cultural issue, or as a sensitive social issue, we should listen to them. I personally agree with them. Our own privacy policy should reflect the socio-cultural mores of our American community as much as our economic system.

I say this to remind ourselves that on a global medium such as the Internet, information about you will not only be of interest to Madison Avenue or your insurance company. As all of us become ever more digital in how we work and play, information about us will become more detailed and more personal in nature, and the ability to create, compile and distribute "digital dossiers" on each of us will become greatly facilitated.

My longstanding interest in privacy comes from my belief that privacy protection is part and parcel of exercising basic civic freedoms and utterly interwoven in our self-identity as Americans. To my mind, losing our privacy altogether would be tantamount to losing our freedom. It is for these reasons that I am honored to be invited to address this conference. And it is for these reasons that I will again battle on Capitol Hill for a strong pro-consumer encryption policy and why I will continue my fight to put basic privacy rules on the books even as we promote new technologies and telecommunications competition.

Children's Privacy

Last year, building upon work done at the Federal Trade Commission (FTC), I offered legislation along with Senator Richard Bryan (D-NV) to protect the privacy rights of kids 12

and under. This measure was ultimately approved by the Congress and is now the law.

The question for us in this session of Congress is whether or not Americans should lose their privacy protections upon turning 13 years of age. While becoming a teenager will always be a rite of passage in America, it must not become the milestone for a flight of privacy.

I believe that any solution to implementing a national privacy policy has to be a combination of 3 key elements: 1) technological tools; 2) industry self-regulation; & 3) a government-enforced set of basic privacy rules.

Let me briefly outline these three elements because I believe that they will ultimately be what our national privacy policy is built upon.

Technological Tools

I have long believed in the potential for technology to help solve some of the problems that technology creates. There is no question that my interest in making sure that strong encryption remains available to all Americans comes from the belief that people ought to be able to take steps themselves to protect their own data, conversations, or intellectual property. Moreover, in the context of online transactional information, the Platform for Privacy Preferences - or "P3P" - certainly holds much promise.

P3P may some day avail consumers of an increased ability to signal electronically to sites on the Web consumers' desires over how such entities should treat their personal information. At the very least, this would save consumers the toil of clicking on the privacy policy of each website they visit in order to ascertain what each site might have in store for their personal data.

Yet this technology can only truly work if it is widely available and if the private sector honors the privacy preferences being expressed by consumers. In addition, as the unveiling of Intel's Pentium III made clear to many of us, relying upon technology alone puts consumer privacy at the trailing edge of a never ending process of technological "one-upsmanship". As consumers get new tools, new challenges are posed to the full and effective utilization of the technological tools.

This is not, in itself, a bad thing. We obviously want technology to evolve. My point is only that personal privacy should not bend to the latest technology, but rather, technology should be designed with privacy in mind. We cannot count on every technology company to do this. And every consumer cannot be expected to be savvy enough about all of the latest gadgetry of the latest products in order to protect themselves. It's an unrealistic expection, which is why we need rules.

As many of you know, I found the unique identifying technology in the Intel Pentium III and Microsoft products very disturbing. I quickly wrote the CEO of Intel when the Pentium III was unveiled to request a redesign of the chip to better address consumer privacy concerns. Many people have come up to me in recent days and have noted that the same unique identifier that causes concern for many privacy advocates and consumers, was critical in tracking down the alleged perpetrator of the Melissa virus.

There is a wringing of hands over the difficulty of reconciling the duality of the technology:

on the one hand it's a threat to privacy and on the other, it may help solve crimes or make transactions more secure.

My response to them is that it is indeed very difficult to reconcile the two - but only if you rely solely upon the technology. If there are no rules that articulate permissible uses and consumer rights then, yes, I tell them, it's quite difficult for consumers to know how to handle this. Again, that's why we need rules. We need rules so companies know how to handle this AND we need rules governing how law enforcement can get access to this information.

Industry Self Regulation

I want to salute the laudable efforts of certain segments of the industry in trying to develop so-called "self-regulatory" solutions. I want to commend thos companies and individuals associated with online privacy initiatives, seal programs such as Trust-E and BBBonline, as well as the growing number of companies taking steps to better inform consumers and offer basic privacy protections on their own initiative.

These undertakings are critical to increasing consumer confidence and trust in the medium and will be an important component in any comprehensive set of privacy protections for consumers.

Many members of the online community have posted privacy policies on their websites in the last year. I am sure that any survey conducted will indicate that there has been a growth in the number of websites that post such privacy policies.

I want to make clear however, that a "posted" privacy policy is not synonymous with a "good" privacy policy.

Everyone who has taken the time and effort to develop and post a privacy policy gets a gold star and a pat on the back.....except, of course those who took the extra time and effort to find the most obscure and remote part of the website to post the notice, with a link in the smallest sized font available, and who then proceeded to "lawyer-up" a plain language privacy notice in a way that would warm the heart of any general counsel.

For any online privacy notice to work, it must be designed to serve consumers by being clear, conspicuous, concise and common sense in its approach. It will not do the industry any good to gleefully trumpet an increase in the number of sites posting privacy notices if it turns out that many of such postings are either hard to find, hard to understand, or both.

In addition, as technology changes, sites will inevitably be able to glean more information electronically and surreptitiously from consumers. In such a context, merely informing consumers that a site may have already gathered personal information electronically and providing notice about how it intends to use such information is unacceptable.

That's like saying burglary is OK as long as the thief leaves behind a note clearly indicating what was stolen and how the thief intends to use the stolen items.

Company executives often ask me, "What if I post on my site a notice about what information I'm gathering and how I'm going to use it - is that OK?" The answer is "Almost"

- a key ingredient is missing: consumer consent. Notice alone is insufficient. Consumers must have an effective opportunity to grant or deny consent.

To be fair, I'm giving a critique of the work of people and companies who are at least trying to be constructive and be part of a solution. Today, our public policy has set up an inverse system of rewards and punishments. If a company takes the time to develop and post a privacy policy and then at some point violates it in some way, the FTC can go after that company and seek to address consumer grievances. On the other hand, if a company posts no policy at all and then engages in personal information hijacking on a daily basis, it is legally free and clear to do just that and continue on its merry way.

That makes no sense. The company without a posted privacy policy is clearly being unfair to consumers and such a legal dynamic is also unfair to all the other companies taking steps to deal forthrightly with consumers. We have got to address this issue. The way to do so is with rules covering all companies and have the FTC enforce them.

My belief is that industry self-regulation is clearly going to be part of any comprehensive privacy policy for the U.S. Consumers should be able to go out and negotiate for better privacy protection in the marketplace and companies ought to compete on terms and conditions of personal information use. But no consumer should be completely bereft of any basic privacy protections when they visit a site.

And again, although I have long been a big believer in utilizing technology to solve some of the problems that technology creates, I don't believe at this time that technological tools will be ubiquitously available and affordable, or universally honored by information hunters and data gatherers to solve the problem through technology alone.

Our national privacy policy must, and I believe inevitably will, include a governmental role. Congress can put rules on the books in a way that factors in new technology, that encompasses what industry self-regulation can offer, but that also deals flexibly, realistically and pragmatically with the limitations of technology and self-regulation in fully protecting consumers.

I do not accept the notion that the Internet is too complex and technology changing so rapidly that we cannot develop enforceable privacy protections for consumers. As technologies change and business plans for online commerce adjust, consumer's privacy principles remain a constant.

In addition to an overarching Privacy Bill of Rights which I just outlined for electronic commerce, I believe it is also essential to enhance the protections offered in two key areas: financial services and health care. I have recently introduced more specific detailed legislation addressing these two areas because I believe financial data and health data warrant a greater degree of protection and I think there is general consensus on that notion.

Today, the convergence of the banking, securities, and insurance industries into giant financial services conglomerates is making it possible to construct a detailed record of a consumer's credit card purchases, checking or savings account deposits or withdrawals, brokerage accounts, mutual fund holdings, and insurance coverage.

If we fail to give financial services consumers effective privacy protections soon, we may

enter a world in which loans are denied when an insurance company informs an affiliated bank that the consumer has a serious medical condition, in which highly vulnerable groups - such as seniors or widows who have just received life insurance beneficiary checks - get cold called by stockbrokers based on information provided by an insurance company or a bank, and in which virtually ever purchase a consumer makes becomes part of a digital dossier that is used for cross-marketing purposes.

Health Privacy

Meanwhile, the lack of a federal law to protect the privacy of our medical records leaves us vulnerable to collapses of confidentiality regarding our most personal and sensitive information.

Recently, the Wall Street Journal wrote about a company that is "seeking the mother lode in health 'data mining.'" The goal of this company is to compile medical data on millions of Americans and to sell this data to any buyer. Everyone's personal health information has become a valuable commodity - to be traded like soybeans or pork bellies - except this commodity contains your family's most personal and intimate secrets.

With no federal law to prevent unfettered access to your medical information, patient confidentiality has become a virtual myth and the sale of your secrets a virtual reality.

The Hippocratic Oath provides that: "All that may come to my knowledge in the exercise of my progression or in daily commerce with men, which ought not to be spread abroad, I will keep secret and will never reveal." I believe this is a firm basis not only for good medicine, but also for good public policy on patient privacy.

But without a federal medical privacy law, not only is your personal information at risk, but also your quality of heath care. We can't let privacy slide to the point where the only way for a person to ensure confidentiality is to avoid medical treatment all together.

While threats to our privacy in this information age compel us to debate the implementation of a medical privacy law, Congress has another reason to address medical privacy. A provision in the Health Insurance Portability and Accountability Act (HIPPA) has imposed an August 19999, deadline for Congress to enact medical privacy legislation. Now is the time to work expeditiously to pass a strong and effective bill.

On March 10th, I introduced the Medical Information Privacy and Security Act of 1999 (MIPSA). MIPSA's companion in the Senate was introduced on the same day by Senators Leahy and Kennedy. This bill provides strong privacy measures while respecting the health care profession's need to share information for treatment and diagnosis. It limits the amount of personal health information required for billing and payment purposes and it gives patients the opportunity to control access to their medical information by third parties. Furthermore, my bill will prevent law enforcement agents from browsing through medical records without a warrant and would close the existing gaps in federal privacy rules to ensure protection of personally identifiable health information by creating a federal floor. The bill would NOT preempt any state law or regulation that offers GREATER privacy safeguards. I propose this for two reasons.

First, a strong federal privacy law will eliminate much of the current patchwork of state laws

governing the exchange of medical information, and will replace the patchwork with strong, clear standards that will apply to everyone.

Second, MIPSA makes room for possible future threats to medical privacy that we may not even anticipate today. As medical and information technology move forward into the next century, we must maintain the public's right to seek stronger medical privacy laws closer to home.

These elements are essential to any strong medical privacy effort.

I want to encourage anyone here today with any thoughts or insights on online privacy or banking privacy or health care privacy to give me a call or contact my staff. I want to especially encourage the online industry to think about how to address privacy for cyberspace in a comprehensive way. Do not wait for a privacy meltdown of Chernobyl-like proportions before you endorse some governmental role. I will be introducing an updated Privacy Bill of Rights legislative initiative in the coming weeks and I would appreciate any input or comments people may have.

Again, thank you very much for the invitation.